Windows NT 4.0 Server Security Assessment Guide

July 9, 2001

Prepared by:
Barre Bull, Sr. IT Security Analyst
Don Truax, HW/SW Installation Tech

1953 Gallows Rd., 2nd Floor
Vienna, VA 22182

SAIC-6099-2001-223

Prepared for:
Mr. Greg Montgomery
U.S. Department of Agriculture
Room 431-W
Whitten Building
14th and Independence
Washington, D.C. 20250

For Official Use Only

U.S. Department of Agriculture

Washington, D.C. 20250

USDA Windows NT Server Security Assessment Guide

1. PURPOSE

This Security Assessment Guide is designed to assist Agency ISSPMs in satisfying their responsibility to develop and implement a comprehensive risk management program as defined in DR 3140-001, "USDA Information Systems Security Policy." By using this guide, Agency ISSPMs can identify areas where Department Information Security requirements are not being met and develop an action plan to ensure all security requirements are satisfied.

2. SCOPE

This guide is to be used by all USDA organizational elements to help assess the security posture of Windows NT 4.0 servers. This checklist is ***not intended to be a configuration guide*** but a tool to assist in determining if the system meets the requirements for a Sensitive But Unclassified (SBU) system and assessing the vulnerabilities, both current and potential, of the system. The checks performed are based on Federal, USDA, and Best Security Practices for the protection of SBU data. This checklist does not address applications installed on the system or special purpose configurations (i.e. web servers, database servers, etc.).

3. BACKGROUND

Risk Assessments are mandated by OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources." A security risk assessment process is a comprehensive evaluation of the system's technical and non-technical security features. It establishes the extent that a specific design and implementation meets specific security requirements.

4. REFERENCES

a. External

(1) Public Law 100-235, "Computer Security Act of 1987"
(2) Public Law 93-579, "Privacy Act of 1974"
(3) Public Law 93-502, "Freedom of Information Act"
(4) Public Law 99-474, "Computer Fraud and Abuse Act"
(5) OMB Circular No. A-130 Appendix III, "Security of Federal Automated Information Resources," revised February 8, 1996.
(6) OMB Circular No. A-123, "Management Accountability and Control," June 29, 1995.

b. USDA Internal Regulations

(1) DR 3140-001, “USDA Information Systems Security Policy” dated may 15, 1996
(2) DM 3140-1 “USDA Management ADP Security Manual” dated March 5, 1992

Windows NT Server Assessment Guide

This assessment should be completed by the Agency's ISSPM or designated alternate in conjunction with the Agency Assessment Checklist. Answer all questions. Provide supplemental information as appropriate. All "No" and "Partial" answers must include supplemental information (such as the given reason why the requirement cannot be met) and an action plan that describes how the requirement will be met, as well as a schedule for completion of the plan. Typically, this would be done by developing the action plan in this document and reflecting this in the security plan for the agency.

Agency/System Identification:

Agency (Agency, Office, Bureau, Service, etc.):	
Address	
Date of last Assessment:	

Test Number: **1**	SITE/SYSTEM:	DATE:	TIME:
Test Name: NT Server Access and Configuration			
Resources Required:	Access to the NT Primary Domain Controller server, Administrative ID and Password for server.		
Personnel Required:	NT Systems Administrator.		
Objectives:	To determine that the NT servers are configured to meet USDA requirements pertaining to systems protection, password policies, user access privileges and virus protection. To determine that file servers are not being used as workstations and that they are located in restricted areas. To determine that all auditing functions are turned on, functioning and properly configured.		
Procedure Description: (Summary)	Verify that access is properly controlled, virus protection software is installed, configured and functioning properly, and that the system policies are configured properly. Verify that file servers are not being used as workstations and that they are located in restricted areas. Verify version and service pack level of operating system.		

Detailed Procedures and Results

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
1.	Ask the System Administrator if the hard drive is formatted using NTFS.	Hard drive is formatted using NTFS.		
2.	Ask the System Administrator if there is an up-to-date Emergency Repair Disk for the system.	There is an up-to-date Emergency Repair Disk for the system.		
3.	Ask the System Administrator if the Emergency Repair Disk is stored in a secure environment.	The Emergency Repair Disk is stored in a secure environment.		
4.	Observe that the system to be assessed is locked or that a password protected screensaver has been implemented.	System is locked or a password protected screensaver is active.		
5.	Ask the System Administrator if the CMOS on all servers are password protected.	The CMOS on all servers are password protected.		
6.	Ask the System Administrator if the server CMOS has been configured to boot only from the hard drive.	The server CMOS has been configured to boot only from the hard drive.		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
7.	Use the Secure Attention Sequence (Ctrl+Alt+Delete) to access the server logon screen.	Logon screen appears.		
8.	Verify that a Legal Notice dialog box appears prior to the Logon dialog box.	A Legal Notice dialog box appears prior to the Logon dialog box.		
9.	Click the OK button in the Legal Notice dialog and continue with log on.	Logon Dialog window is presented on screen.		
10.	Verify that there is no User ID from a previous session in the User ID portion of the logon window.	There is no User ID from a previous session in the User ID portion of the logon window.		
11.	Observe how many buttons are at the bottom of the logon window.	3 buttons are on the logon window, the Logon button, Cancel button and Help button. The Shutdown button should be grayed out.		
12.	Ask the SA if the Guest account has a password.	Guest account has a password.		
13.	Attempt to logon to the system using the User ID Guest and pressing return (do not enter a password).	Access denied.		
14.	Attempt to logon to the system using the User ID Guest and enter Guest for the password.	Access denied.		
15.	Attempt to logon to the system using the User ID Administrator and pressing return (do not enter a password).	Access denied.		
16.	Attempt to (or have system administrator) logon to the system using the administrative User ID and entering the administrative password.	Logon in Process message window appears.		
17.	Ask the System Administrator if local or centralized virus scanning is used.	If local virus scanning is used skip to question 19.		
18.	If centralized virus scanning is used ask the System Administrator if the virus signatures are kept current on the central scanning system.	Most current version of the virus signatures is being used. Skip to question 21		
19.	When the desktop appears observe the system tray in the bottom right corner of the desktop to verify that a virus	Virus protection software icon is present.		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
	protection software icon is present.			
20.	Have SA show the date of the virus patterns/signatures currently running.	The patterns/signatures should be no more than one month old.		
21.	Right click on the desk top and select Properties	Display Properties window opens.		
22.	Select the Screen Saver tab.	♦ A screensaver has been selected. ♦ The Password Protected box is checked. ♦ The Wait time is set to a maximum of 15 minutes.		
23.	Close Display Properties window.	Display Properties window closes.		
24.	Click on the Start menu button in the task bar.	Start menu choices appear.		
25.	Click on the Programs selection.	Program menu appears.		
26.	Select Administrative Tools (Common).	Administrative Tools menu appears.		
27.	Select User Manager for Domains.	User Manager for Domains window opens.		
28.	Observe that the Administrator account has been renamed.	Administrator account has been renamed.		
29.	Ask the SA if the Administrator account is used.	Administrator account is not used.		
30.	Ask the SA if users requiring administrative access to servers have individual accounts with membership in the Administrators Group.	Users requiring administrative access to servers have individual accounts with membership in the Administrators Group.		
31.	Double click the Guest account to view its properties.	Guest account properties dialog window opens.		
32.	Observe that the User Cannot Change Password, Password Never Expires and Account Disabled boxes are checked.	User Cannot Change Password, Password Never Expires and Account Disabled boxes are checked.		
33.	Click on the Groups button in the Guest account properties window and observe what groups the Guest account is a member of.	Guest account is a member of no Groups.		
34.	Close Guest account properties window.	Guest account properties dialog window		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
		closes.		
35.	Ask SA if system rights/permissions are assigned based on Group membership of users.	Rights/permissions are assigned based on Group membership of users.		
36.	Ask SA if system rights/permissions are assigned to groups or individual users.	Rights/permissions are assigned to groups not individual users.		
37.	Ask SA if users are assigned to groups based on job function and/or "need to know."	Users are assigned to groups based on job function and/or "need to know."		
38.	Observe Groups listing in the User Manager to ensure approved Groups exist.	Approved Groups exist.		
39.	Exit the User Manager for Domains Menu.	User Manager for Domains Menu closes.		
40.	Ask the SA if the file servers are used as workstations and observe that physical access is restricted.	File servers are not used as workstations and physical access to the file servers is restricted.		
41.	Open Start menu, select Programs and observe the programs listed.	There are no programs listed that are not necessary to the functioning of the server.		
42.	Ask the SA if shared system and security software files are protected from unauthorized access and modification.	Shared system and security software files are protected from unauthorized access and modification.		
43.	Open Start menu and click on Settings	Settings menu appears.		
44.	Click on Control Panel	Control Panel window opens		
45.	Click on the Control Panel Help menu and select About Windows NT	About Windows NT window opens.		
46.	Verify that Version 4.0 of Windows NT is the current version of the operating system.	The operating system is Windows NT 4.0		
47.	Verify that the current Service Pack is installed.	The current Service Pack has been installed.		
48.	Ask SA if unnecessary services have been disabled.	Unnecessary services have been disabled. (Unnecessary services will be different from system to system in some cases and will generally be determined locally.)		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
49.	Exit the Help window and exit the Control Panel.	Help and Control Panel windows close.		

Comments:
Action Plan:

Test Number: **2**	SITE/SYSTEM:	DATE:	TIME:
Test Name: NT PDC Server Password Policy Configuration			
Resources Required:	Access to the NT Primary Domain Controller with Administrator Access		
Personnel Required:	NT Systems Administrator.		
Objectives:	To determine that the NT Password Policies are configured to meet USDA requirements pertaining to Identification and Authentication.		
Procedure Description: (Summary)	Verify that Password Policies are properly configured.		

Detailed Procedures and Results

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
1.	Open the User Manager for Domains from the Start/Programs/Administrative Tools Common menu.			
2.	Click on the Policies menu button at the top of the User Manager for Domains window and select Account.	Account settings screen appears.		
3.	Verify that the account policies match those on the NT Account Policy settings attachment.	The account policies match those on the NT Account Policy Settings attachment.		
4.	Maximum password age is set to 90 days	Maximum password age is set to 90 days		
5.	Minimum password age allows change after 7 days	Minimum password age allows change after 7 days		
6.	Minimum password length is set to 6 characters	Minimum password length is set to 8 characters		
7.	Password Uniqueness is set to remember 5 passwords	Password Uniqueness is set to remember 5 passwords. (**NOTE**: the Password Uniqueness box will show 3. NT remembers 2 passwords by default and putting 3 in the box will make it a total of 5.)		
8.	Lock Out is set to lock out after 3 failed login attempts	Lock Out is set to lock out after 3 failed login		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
		attempts		
9.	Lock out is set to reset count after 60 minutes	Lock out is set to reset count after 60 minutes		
10.	Lock out duration is set to Forever – Until unlocked by Administrator	Lock out duration is set to Forever – Until unlocked by Administrator		
11.	Click OK.	Account settings screen closes.		

Comments:
Action Plan:

Test Number: **3**	SITE/SYSTEM:	DATE:	TIME:
Test Name: NT Server Registry Settings			
Resources Required:	Administrative access to the NT Domain Controller.		
Personnel Required:	NT System Administrator.		
Objectives:	To verify that all registry settings in place and correctly configured.		
Procedure Description: (Summary)	Using Regedt32, access the system registry and verify that specific registry keys are correctly configured. **WARNING: This test must be done carefully to prevent any damage to the registry. DO NOT ATTEMPT TO EDIT THE REGISTRY!**		

Detailed Procedures and Results

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
1.	Click on the Start button in the Task Bar.	Start menu choices appear.		
2.	Click on Run.	Run Dialog window opens.		
3.	Enter Regedt32 in the Run dialog.	Regedt32 starts and the Registry tree appears in the left window.		
4.	Select the HKEY_LOCAL_MACHINE folder.	Hive categories appear.		
5.	Click on Security at the top and select Permissions	Registry Permissions dialog window opens		
6.	Ensure Permissions are correct.	Administrators-Full Control Everybody-Read Only System-Full Control NOTE: The box "Replace Permissions on Existing Subkeys" is NOT checked.		
7.	Exit Permissions dialog window	Permissions dialog window closes		
8.	Select Software\Microsoft\Windows NT\CurrentVersion\Winlogon. Observe the LegalNoticeCaption in the right side of the window and verify that the text string within the double quotes is "AUTHORIZED USE ONLY."	The text string within the double quotes is "AUTHORIZED USE ONLY."		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
9.	Observe the LegalNoticeText in the right side of the window and verify that the text within the double quotes is equivalent to the text in Attachment 1.	The text within the double quotes is equivalent to the text in the Attachment 1.		
10.	Observe the DontDisplayLastUserName entry in the right window and verify that a "1" appears in the double quotes.	A "1" appears in the double quotes.		
11.	Verify that the ShutdownWithoutLogon value is set to 0.	ShutdownWithoutLogon value is set to 0.		
12.	Select \Microsoft\OS/2 Subsystem for NT and ensure that it contains no subkeys.	\MicrosoftOS/2 Subsystem for NT contains no subkeys.		
13.	Select \Program Groups window, then select the "Security", and "Auditing" menu choices.	Significant changes are audited.		
14.	Select HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NotificationPackages has the string passfilt.dll listed.	\NotificationPackages has the string passfilt.dll listed. **Note:** passfilt.dll forces password complexity.		
15.	Select HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA. The RestrictAnonymous should be present and the value should be set to 1.	RestrictAnonymous has been created and the value is 1. **Note**: This setting restricts anonymous users from being able to obtain public information about the LSA component of the Windows NT Security Subsystem. The LSA handles aspects of security administration on the local computer, including access and permissions.		
16.	Select HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Subsystems and verify there are no entries for Posix and OS/2	There are no entries for Posix and OS/2. **Note:** These subsystems were not included in the evaluated configuration, and therefore C2-like		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
		compliance cannot be achieved unless they are removed.		
17.	Select HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters and verify that EnablePortLocking has been added and set to a value of 1.	EnablePortLocking has been added and set to a value of 1. **Note:** An unprivileged user mode application should not be able to listen to TCP and UDP ports used by Windows NT services, regardless of the cryptographic protection applied to the Windows NT service traffic through the ports.		
18.	Select HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\GraphicsDrivers\DCI\Timeout and verify that the value is set to 0.	Timeout value is set to 0. **Note:** This prevents direct access to video hardware and memory.		
19.	Select HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\ ProtectionMode and verify that the value is set to 1.	ProtectionMode value is set to 1. **Note:** This setting is necessary to further heighten security of the base objects. Among other things, it prevents users from gaining local administrator privileges by way of a dynamic-link library (DLL).		
20.	Select HKEY_LOCAL_MACHINE\SYSTEM\Optional and verify that there are no values listed.	HKEY_LOCAL_MACHINE\SYSTEM\Optional does not exist or No values are listed.		
21.	Click on the window "HKEY_CLASSES_ROOT". Select "Security", then "Permissions" from the menu.	Verify that permissions on "HKEY_CLASSES_ROOT" and all its subkeys are set to: Administrators - Full Control CREATOR OWNER - Full Control Everyone - Read System - Full Control		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
		NOTE: The box "Replace Permissions on Existing Subkeys" is NOT checked.		
22.	Select "HKEY_USERS" and the folder "HKEY_USERS\.DEFAULT \UNICODE Program Groups\". Select "Security", then "Permissions" from the menu.	Verify that permissions on "HKEY_USERS\.DEFAULT \UNICODE Program Groups\[all subkeys]" are set to: Administrators - Full Control Everyone - Read System - Full Control		
23.	Exit Regedt32			

Comments:

Action Plan:

Test Number: **4**	SITE/SYSTEM:	DATE:	TIME:
Test Name: NT Server Audit			
Resources Required:	Access to the NT Primary Domain Controller or server with Administrator Access		
Personnel Required:	NT Systems Administrator.		
Objectives:	To determine that the NT servers are configured to meet USDA requirements pertaining to Auditing.		
Procedure Description: (Summary)	Verify that auditing is turned on, functioning and properly configured. Also, verify that the audit logs are reviewed on a regular basis and backed up on a regular schedule.		

Detailed Procedures and Results

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
1.	Ask the SA if there is a documented schedule for the review of Audit logs.	Audit logs are reviewed per documented schedule.		
2.	Ask the SA if the audit logs are backed up according to a routine schedule. Observe back-ups of audit logs.	Audit logs are backed up according to a routine schedule.		
3.	Ask the SA if there are procedures in place for moving the logs off the system when they become full.	There are procedures in place for moving the logs off the system when they become full.		
4.	Ask the SA if copies of the audit log backups are stored in a secure environment offsite.	Copies of the audit log backups are stored in a secure environment offsite.		
5.	Click on the Start menu button in the task bar.	Start menu choices appear.		
6.	Click on the Programs selection.	Program menu appears.		
7.	Select Administrative Tools (Common).	Administrative Tools menu appears.		
8.	Select User Manager for Domains.	User Manager for Domains window opens.		
9.	Select the Policies menu at the top of the User Manager for Domains window and select Audit.	Audit settings screen appears.		
10.	Verify that the Audit These Events option is selected.	Audit These Events option is selected.		
11.	Verify that all events are selected for Success and Failure except Process Tracking, which only has	All events are selected for Success and Failure except Process Tracking, which only		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
	Failure selected. (See Attachment 3)	has Failure selected.		
12.	Click OK.	Audit settings screen closes.		
13.	Click the Start button in the task bar.	Start menu choices appear.		
14.	Select Programs.	Programs menu appears.		
15.	Select Administrative Tools (Common).	Administrative Tools menu appears.		
16.	Select Event Viewer.	Event Viewer window opens.		
17.	At the top of the Event Viewer window click on the Log menu selection.	Log menu appears.		
18.	Select the System Log.	System log appears in window.		
19.	Click on the log menu again and select Log Settings.	System log settings dialogue appears.		
20.	Verify that “Do Not Overwrite” box is checked.	“Do Not Overwrite” box is checked.		
21.	Click OK on Log Settings Dialogue.	Log Settings Dialogue window closes.		
22.	At the top of the Event Viewer window click on the Log menu selection.	Log menu appears.		
23.	Select the Application Log.	Application log appears in window.		
24.	Click on the log menu again and select Log Settings.	Application log settings dialogue appears.		
25.	Verify that “Do Not Overwrite” box is checked.	“Do Not Overwrite” box is checked.		
26.	Click OK on Log Settings Dialogue.	Log Settings Dialogue window closes.		
27.	At the top of the Event Viewer window click on the Log menu selection.	Log menu appears.		
28.	Select the Security Log.	Security log appears in window.		
29.	Click on the log menu again and select Log Settings.	Security log settings dialogue appears.		
30.	Verify that “Do Not Overwrite” box is checked.	“Do Not Overwrite” box is checked.		
31.	Click OK on Log Settings Dialogue.	Log Settings Dialogue window closes.		
32.	Close Event Viewer window.	Event Viewer window closes.		

Comments:

Action Plan:

Test Number: **5**	SITE/SYSTEM:	DATE:	TIME:
Test Name: NT Server System Backups			
Resources Required:	Access to the NT Primary Domain Controller server (or server used for backups) with Administrator Access		
Personnel Required:	NT Systems Administrator.		
Objectives:	To ensure that NT Server operating systems and applications are backed up on a timely basis and that backup procedures are being performed.		
Procedure Description: (Summary)	Examine backup scheduler program and log files to determine that backups are conducted on a timely basis. Review NT Server backup procedures and determine that procedures are being performed. Ensure that copies of back-ups are stored off-site.		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
1.	Log onto NT as Administrator.	Successful log-on.		
2.	Review backup scheduler programs and log files to determine that backups are conducted on a timely basis.	Backups are conducted on a timely basis.		
3.	Ask Administrator for Server backup procedures document and ask if the procedures are being followed.	Server backup procedures documentation available and procedures are being performed as required.		
4.	Ask Administrator if backup software updates and patches are current.	Backup software updates and patches are current.		
5.	Ask Administrator if server backups are tested.	Server backups are tested.		
6.	Ask SA if copies of backups are stored off-site, in a secure environment, on a regular basis.	Copies of backups are stored off-site, in a secure environment on a regular basis.		

Comments:
Action Plan:

ATTACHMENT 1

Legal Notice Text string:

UNAUTHORIZED ACCESS TO THIS UNITED STATES GOVERNMENT COMPUTER SYSTEM AND SOFTWARE IS PROHIBITED BY PUBLIC LAW 99-474, TITLE 18, UNITED STATES CODE. PUBLIC LAW 99-474 AND CHAPTER XXI, SECTION 1030 STATES THAT…

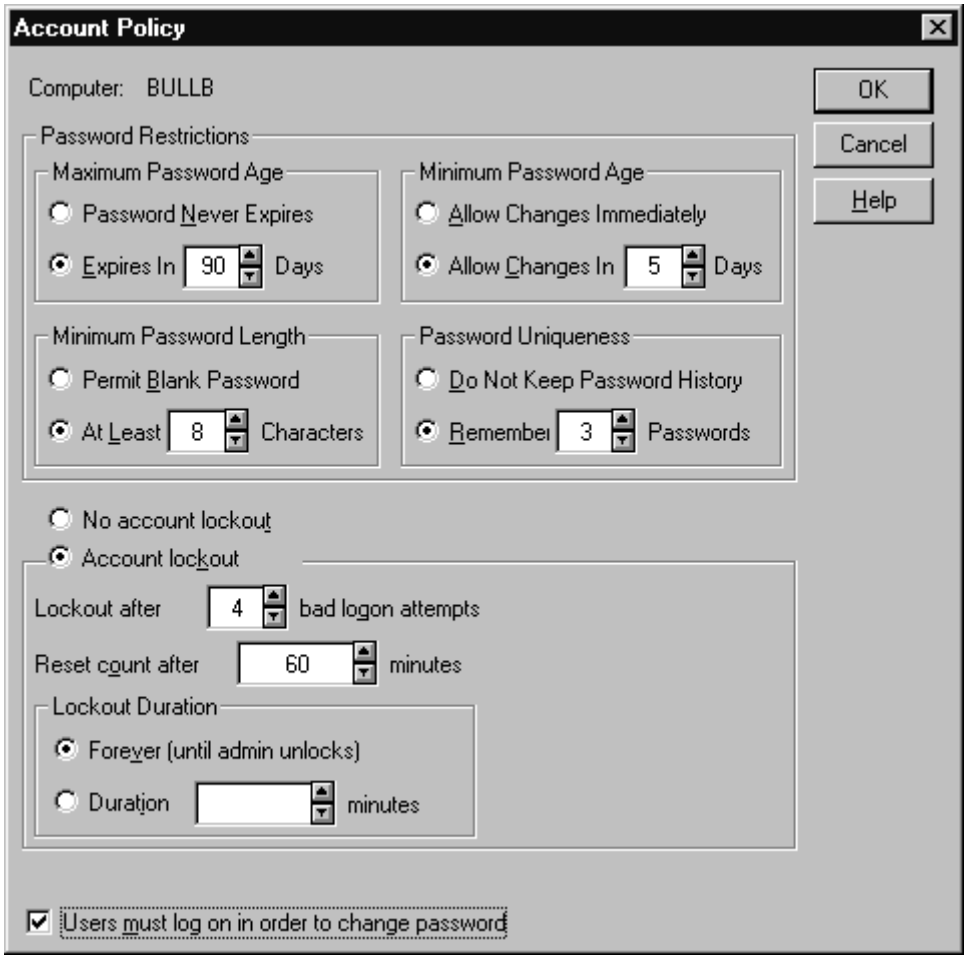
Whoever knowingly, or intentionally accesses a computer without authorization or exceeds authorized access, and by means of such conduct, obtains, alters, damages, destroys, or discloses information, or prevents authorized use of (data or a computer owned by or operated for) the Government of the United States, shall be punished by a fine under this title or imprisonment for not more than 10 years, or both.

All activities on this system may be recorded and monitored. Individuals using this system expressly consent to such monitoring. Evidence of possible misconduct or abuse may be provided to appropriate officials.

REPORT UNAUTHORIZED USE TO AN INFORMATION SYSTEMS SECURITY OFFICER

ATTACHMENT 2

NT Domain Account Policy Settings



ATTACHMENT 3

Audit Policy Settings: